



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,509	03/28/2001	Mahfuzur Rahman	MAT1-202US	4790
23122	7590	11/16/2004	EXAMINER	
RATNERPRESTIA			FIELDS, COURTNEY D	
P O BOX 980			ART UNIT	
VALLEY FORGE, PA 19482-0980			PAPER NUMBER	

2137

DATE MAILED: 11/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/819,509

Applicant(s)

RAHMAN ET AL.

Examiner

Courtney D. Fields

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 March 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 28 March 2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.
2. The Information Disclosure Statement respectfully submitted on 28 March 2001 has been considered by the Examiner.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Baird, III et al. (U.S. Patent No. 6, 732,278). Referring to the rejection of claims 1 and 16, Baird, III et al. discloses a method and computer program for forming a strong password comprising the steps of: obtaining biometric data from a user, generating a one-time password for the user, and combining the biometric data and the one-time password to form the strong password in Column 6, lines 35-48, Column 8, lines 22-58.

As per claims 2 and 17, Baird, III et al. discloses the claimed limitation wherein comprising the step of encrypting the combined one-time password and biometric data using an encryption key to form the strong password in Column 13, lines 45-57.

Referring to the rejection of claims 3 and 18, Baird, III et al. discloses a method and computer program for controlling access to secure data comprising the data from a user, separating the one-time password and the biometric data, comparing the one-time password and the biometric data, comparing the one-time password to a calculated one-time password to determine if the one-time password is valid, determining a probability that the biometric data is from the user, encrypting the secure data using an encryption key to obtain encrypted data if the one-time password matches the calculated one-time password and the probability that the biometric data is from the user exceeds a predetermined threshold value, combining the strong password, the encryption key and the encryption data, and transmitting the combined strong password, encryption key and encrypted data to the user in Column 16, lines 61-67, Column 17, lines 1-67, and Column 18, lines 1-12.

As per claims 4 and 19, Baird, III et al. discloses the claimed limitation wherein the step of encrypting the combined strong password and encryption key using a further encryption key in Column 9, lines 52-67, Column 10, lines 1-17.

As per claims 5 and 20, Baird, III et al. discloses the claimed limitation wherein the secure data includes items having respectively different security levels, and the step of encrypting the secure data aborts the method if either the one-time password does not match the calculated one-time password or the probability that the biometric data is

from the user does not exceed the predetermined threshold value in Column 12, lines 10-13, Column 17, lines 32-65.

Referring to the rejection of claim 6, Baird, III et al. discloses a system for implementing secure access to a remote computer system comprising: at least one first computer securely coupled to the remote computer system, at least one second computer coupled to the at least one first computer and configured to obtain identifying information from a user, whereby the second computer passes the identifying information to the first computer, the first computer passes the identifying information to the remote computer system and the remote computer system verifies the identifying information in Column 10, lines 60-67, Column 11, lines 1-28.

As per claim 7, Baird, III et al. discloses the claimed limitation wherein the identifying information is a strong password including a one-time password and biometric information in Column 6, lines 35-48.

As per claim 8, Baird, III et al. discloses the claimed limitation wherein the identifying information is encrypted with an encryption key in Column 13, lines 54-57, Column 19, lines 1-5.

As per claim 9, Baird, III et al. discloses the claimed limitation wherein the second computer is securely connected to the first computer by means of a Secure Socket Layer connection in Column 12, lines 15-19.

As per claim 10, Baird, III et al. discloses the claimed limitation wherein the second computer includes a further Secure Socket Layer connection for receiving the identifying information from the user in Column 12, lines 19-28.

As per claim 11, Baird, III et al. discloses the claimed limitation wherein the remote computer includes firewall software through which the first computer is coupled to a remote computer in Column 4, lines 19-53.

Referring to the rejection of claim 12, Baird, III et al. discloses a method of allowing access to secure data on a remote computer including the steps of: receiving a request from a user to access the secure data at a first computer, transferring the request to access the secure data from the first computer, transferring the request to access the secure data from the first computer to the second computer, transferring the request to access the secure data from the second computer to the remote computer, authorizing access to the secure data at the remote computer, transferring the secure data from the second computer to the user without using the first computer in Column 14, lines 5-30.

As per claim 13, Baird, III et al. discloses the claimed limitation wherein the request to access the secure data includes a strong password and the steps of: encrypting the secure data with an encryption key, combining the encryption key with the strong password, encrypting the combined encryption key and the strong password with a further encryption key and transferring the encrypted combined encryption key and strong password and the encrypted secure data to the second computer in Column 13, lines 45-67, Column 14, lines 1-30.

As per claim 14, Baird, III et al. discloses the claimed limitation wherein the step of encrypting the combined password and strong password with an asymmetric encryption key in Column 9, lines 52-67, Column 10, lines 1-17.

As per claim 15, Baird, III et al. discloses the claimed limitation wherein the steps of: separating the one-time password and the biometric information, comparing the one-time password to a calculated one-time password, determining a probability that the biometric information matches an authorized user and authorizing access to the secure data only if the one time password matches the calculated one-time password and the probability that the biometric information matches an authorized user exceeds a predetermined threshold value in Column 16, lines 61-67, Column 17, lines 1-67, and Column 18, lines 1-12.

Conclusion

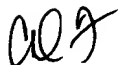
3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Kaliski, Jr. (Pub No. US2001/0055388) discloses a method and system for regenerating a strong secret from a weak secret.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



cdf
October 31, 2004


Andrew Caldwell